Amendments to the Claims

1. (currently amended) A cryptography accelerator, comprising:

a plurality of input ports configured to receive a data sequence comprising header information and payload information from an entity external to the cryptography accelerator;

a plurality of cryptographic processing cores, each cryptographic processing core having a plurality of data paths;

~~a shared~~ an input buffer ~~associated with a~~ shared among the plurality of input ports and the plurality of data paths associated with each cryptographic processing core in the plurality of cryptographic processing cores, the shared input buffer configured to hold payload information associated with the data received by the plurality of input ports; and

a security association lookup unit configured to identify a security association address in a first portion of ~~the~~ an address space associated with the cryptography accelerator by using header information, the first portion of the address space corresponding to bus controller memory, wherein the security association lookup unit is operable to acquire the security association information from bus controller memory.

2. (original) The cryptography accelerator of claim 1, wherein the security association lookup unit identifies the security association address using header information associated with the received data sequence.

3. (original) The cryptography accelerator of claim 2, wherein the security association lookup unit identifies the security association address by performing a hash on the header information.

4. (original) The cryptography accelerator of claim 2, wherein the security association lookup unit identifies the security association address by performing a hash using a source address, a destination address, a SPI, a source port number, and a destination port number.

5. (original) The cryptography accelerator of claim 4, wherein the hash further uses protocol information and a version number.

6. (previously presented) The cryptography accelerator of claim 1, wherein the first portion of the address space is associated with a HyperTransport interconnect system.

7. (original) The cryptography accelerator of claim 1, wherein the first portion of the address space is a Peripheral Components Interface (PCI) address space.

8. (original) The cryptography accelerator of claim 7, wherein a second portion of the address space corresponds to a system memory address space, the random access memory coupled to a CPU external to the cryptography accelerator.

9. (original) The cryptography accelerator of claim 8, wherein a third portion of the address space corresponds to onchip memory.

10. - 11. (canceled)

12. (currently amended) A cryptography accelerator, comprising:

a data input unit, wherein the data input unit includes:

a plurality of input ports, one or more input ports configured to receive a data packet,

a plurality of cryptographic processing cores, each cryptographic processing core having a plurality of data paths, and

an input buffer shared among the plurality of input ports and the plurality of data paths associated with each cryptographic processing core in the plurality of cryptographic processing cores; and

a policy security association lookup unit configured to issue a read request to a bus controller memory for security association information for a first data packet and to process a second data packet prior to receipt of the read response for the first data packet, wherein the bus controller memory is separate from a system memory.

13. (previously presented) The cryptography accelerator of claim 12, further comprising:

a plurality of cryptographic processing data paths coupled to the data input unit, wherein each data path includes a cryptographic processing core.

14. (previously presented) The cryptography accelerator of claim 12, wherein the policy security association lookup unit is configured to derive a security

association handle for the first data packet using header information associated with the first data packet.

15. (previously presented) The cryptography accelerator of claim 12, wherein the policy security association lookup unit receives a security association handle for the first data packet from the data input unit.

16. (previously presented) The cryptography accelerator of claim 13, further comprising:

a merge data unit coupled to the data input unit, the policy security association lookup unit, and a set of the plurality of cryptographic processing data paths, wherein the merge data unit is configured to merge payload data, header information, and security association information associated with the first data packet.

17. (previously presented) The cryptography accelerator of claim 16, wherein the merge data unit is further configured to select one of the cryptographic processing data paths in the set of the plurality of cryptographic processing data paths and to transmit the merged data to the selected cryptographic processing data path.

18. (previously presented) The cryptographic accelerator of claim 12, wherein the bus controller memory is memory associated with a Peripheral Components Interface (PCI) bus.

19. (previously presented) The cryptographic accelerator of claim 12, wherein the bus controller memory is memory associated with a HyperTransport interconnect system.